# A computer scientist point of view on Hilbert's differential theorem of zeros*

François Boulier, François Lemaire
Université Lille I, LIFL, 59655 Villeneuve d'Ascq, France

September 9, 2007

**Abstract**

What is a solution of a system of polynomial differential equations ? This paper provides an original presentation of well-known theorems, with a computer scientist flavor, relying on an improved normal form algorithm.

*Keywords* computer algebra; differential algebra; theorem of zeros; normal form; Rosenfeld-Gröbner

*AMS Classification* 12H05

## 1 Introduction

According to the reference book [32] on *differential algebra* by Ritt, a solution (or a zero) of a polynomial differential system $\Sigma$ in $n$ differential indeterminates, $m$ derivations, with coefficients in some differential field of characteristic zero (say, the field $\mathbb{Q}$ of the rational numbers for simplicity), is *not* a $n$-tuple of functions depending on $m$ variables but a $n$-tuple of quantities living in some differential field extension of the base field of $\Sigma$ which annihilates the system. One refers to such a solution as an *abstract solution* in this paper. This viewpoint is actually the analogue of the classical viewpoint for usual (non differential) polynomial systems: a solution of a polynomial system in $n$ indeterminates and coefficients in $\mathbb{Q}$ is a $n$-tuple of values taken in some finite field extension of $\mathbb{Q}$ or, more simply, in the field $\mathbb{C}$ of the complex numbers since every finite field extension of $\mathbb{Q}$ can be embedded in $\mathbb{C}$. Indeed, Ritt wrote in his preface that his presentation of differential algebra was deeply influenced by the works of Emmy Nœther in the 1920's. However, the theory is much less intuitive in differential than in non differential algebra. In particular, the *universal differential field extensions* which would play, in the differential setting, the role of the field $\mathbb{C}$, are much less familiar than $\mathbb{C}$ for the majority of scientists. See [18, chap. III] or [11, sect. 1.5]. In his founding book, Ritt does not neglect the point of view of Analysis

*Submitted to *Foundations of Computational Mathematics*.

(this is a difference with the reference book [18] of Kolchin) but he presents it rather quickly: he presents in sequence, the systems of differential polynomials, a theory for *differential polynomial ideals*, abstract solutions and writes, page 23 of his book, that all the given definitions and arguments *retain their validity, in the analytic case* i.e. with solutions of differential polynomial systems sought as $n$-tuples of meromorphic functions.

Differential algebra, which was thought by Ritt and Kolchin, as a pretty abstract theory, does have applications: there exists algorithms dedicated to the elimination theory in differential polynomial ideals which are nowadays implemented in computer algebra software. In particular, the *Rosenfeld-Gröbner* algorithm [5, 6, 7] is implemented in the MAPLE *diffalg* package and in the BLAD libraries [2]; related methods can also be found in [35, 40, 23, 30, 22, 13, 10]. These methods apply in various areas: eliminating the variables for which no measures are available simplifies the parameters estimation problem [27]; computing the underlying explicit differential system and the hidden algebraic constraints permits to reduce the differentiation index of differential-algebraic equations [29] while performing the simplifications which follow the quasi-steady state approximations simplifies model reductions [4].

This paper actually aims at widening the audience of these new methods. To reach this goal, it presents what a solution of a differential polynomial system is, in a more computational hence, perhaps, in a less abstract way: instead of defining *a priori* what a solution is and deducing afterwards the authorized algorithmic manipulations, one first states the very simple algorithmic manipulations carried out by the above methods and one deduces afterwards the necessary conditions that any definition of solution must satisfy in order to be compatible with these methods. As we shall see, at least three definitions fit: the abstract solutions, the formal power series solutions and the analytic solutions. For analytic solutions, one relies on a result [19] of Lemaire, though the material is known since the works [31, 36] of Riquier and Seidenberg. Lemaire's formulation, which is more modern, provides a better separation between the construction of formal power series and the convergence theorem. The presentation of formal power series solutions gives us the opportunity to recall a normal form algorithm which permits us to compute in algebraic structures defined by differential generators and relations. This paper provides a better exposition for this important algorithm, which was formerly presented too briefly in [8, sect. 8]. The second item of our Proposition 2 is new while our Lemma 3 clarifies the existing relationship between the zeros of the denominators of normal forms and those of initials and separants of characteristic sets.

## 2 Basics of differential algebra

The reference books are that of Ritt and Kolchin [18, 32]. More recent texts are [11, 38, 39, 14]. A *differential ring* $R$ is a ring endowed with finitely many, say $m$, abstract *derivations* $\delta_1, \ldots, \delta_m$ i.e. unary operations which satisfy the

following axioms:

$$\delta(a+b) = \delta(a) + \delta(b), \quad \delta(a\,b) = \delta(a)\,b + a\delta(b), \qquad (\forall\ a,\ b \in R)$$

and which are assumed to commute pairwise. This paper is mostly concerned by a differential polynomial ring $R$ in $n$ *differential indeterminates* $u_1, \ldots, u_n$ with coefficients in a commutative differential field $K$ of characteristic zero, say $K = \mathbb{Q}$. Letting $U = \{u_1, \ldots, u_n\}$, one denotes $R = K\{U\}$, following Ritt and Kolchin. The $u_i$ can be thought of as the unknown functions of the differential equations but, at this stage, they are plain symbols. The set of derivations generates a commutative monoid w.r.t. the composition operation. It is denoted:

$$\Theta = \{\delta_1^{a_1} \cdots \delta_m^{a_m} \mid a_1, \ldots, a_m \in \mathbb{N}\}$$

where $\mathbb{N}$ stands for the set of the nonnegative integers. The elements of $\Theta$ are the *derivation operators*. If $\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$ is a derivation operator then $\operatorname{ord}\theta = a_1 + \cdots + a_m$ denotes its *order*. The monoid $\Theta$ acts on $U$, giving the infinite set $\Theta U$ of the *derivatives*. One indices derivations with letters e.g. $\delta_x$, $\delta_y$ and one denotes derivatives using subscripts e.g. $u_{xy}$ denotes $\delta_x\,\delta_y\,u$.

An important construction in the rings theory is that of ideals for it permits to build factor rings of a ring $R$ and, when $R = K[X]$ is a polynomial ring over a field $K$, to build field extensions of $K$. One defines *differential ideals* in the differential rings theory for a similar purpose. By definition, a *differential ideal* $\mathfrak{A}$ of a *differential ring* $R$ is an ideal of $R$ which is stable under the action of derivations: $a \in \mathfrak{A} \Rightarrow \delta a \in \mathfrak{A}$ for all $a \in R$ and derivation $\delta$. Since the concept of factor ring is central in this paper, let us briefly introduce it, for casual readers, starting by analogy with the ring $\mathbb{Z}$ of the integer numbers. If $n$ is a nonzero integer, $\mathbb{Z}/n\mathbb{Z}$ denotes the set of the $n$ residue classes of the equivalence relation modulo the ideal $n\mathbb{Z}$ of $\mathbb{Z}$. The set $\mathbb{Z}/n\mathbb{Z}$ is endowed with a ring structure by letting (the "bar" stands for "residue class")

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a} \times \overline{b} = \overline{a \times b}.$$

This definition makes sense for the class of $a+b$ (resp. $a \times b$) only depends on the classes, not on the chosen representatives. If $\mathfrak{A}$ is an ideal of a ring $R$, one defines the factor ring $R/\mathfrak{A}$ exactly the same way. Now, if $\mathfrak{A}$ is a differential ideal of a differential ring $R$, the factor ring $R/\mathfrak{A}$ can be endowed with derivations (indeed, as many derivations as $R$ has), thereby becoming a differential ring, by letting $\delta\overline{a} = \overline{\delta a}$. Again, the definition makes sense because the ideal is differential: the class of $\delta a$ only depends on the class of $a$, not on $a$ [18, chap. I, §2].

If $A$ is a finite subset of $R$, one denotes $(A)$ the smallest ideal containing $A$ w.r.t. the inclusion relation and $[A]$ the smallest differential ideal containing $A$. If $\mathfrak{A}$ is an ideal, then $\sqrt{\mathfrak{A}}$, which is called the *radical* of $\mathfrak{A}$, is the set of all the ring elements a power of which lies in $\mathfrak{A}$ [41, chap. III, §7]. The radical of a (differential) ideal is a (differential) ideal [32, chap. I, §9]. A radical (*perfect* in the Ritt-Kolchin terminology) ideal is an ideal equal to its radical. If $S = \{s_1, \ldots, s_t\}$ is a finite subset of $R \setminus K$ then

$$\mathfrak{A} : S^\infty = \{p \in R \mid \exists\ a_1, \ldots, a_t \in \mathbb{N},\ s_1^{a_1} \cdots s_t^{a_t}\, p \in \mathfrak{A}\}$$

is called the *saturation* of $\mathfrak{A}$ by the multiplicative family generated by $S$. The saturation of a (differential) ideal is a (differential) ideal [18, chap. I, Corollary to Lemma 1].

# 3 Two inference rules and a theorem

Throughout this paper, $\Sigma$ denotes a finite subset of the polynomial differential ring $R = K\{U\}$ endowed with $m$ abstract derivations $\delta_1, \ldots, \delta_m$. Naively, a *solution* of $\Sigma$ is a $n$-tuple of "values" which, when substituted in the equations of $\Sigma$, annihilate them. We are concerned by the type of algebraic structure $G$ in which these values can lie. The differential elimination methods cited in the introduction rely on two inference rules and one theorem. The inference rules are, for all differential polynomials $p$, $q \in R$:

1. $p = 0 \Rightarrow \theta p = 0$ where $\theta p$ denotes a derivative of $p$ of any order,
2. $p\,q = 0 \Rightarrow [p = 0 \text{ or } q = 0]$.

The key theorem is a Nullstellensatz. See [32, chap. I, §16] or [34, sect. 4]. See [41, chap. VII, §3, Theorem 14] for the classical non differential version.

**Theorem 1** *(Nullstellensatz) Every radical differential ideal of $R$ is an intersection of prime differential ideals.*

To enlighten the consequences of the inference rules, let us take for first example an ordinary polynomial differential system made of a unique equation, a famous example [32, chap. II, example 1] of Ritt:

$$u_x^2 - 4\,u = 0.$$

The first inference rule implies that one does not change the solutions of this system by augmenting it with the infinite set of the derivatives of the equation:

$$u_x^2 - 4\,u = 0, \quad 2\,u_x\,u_{xx} - 4\,u_x = 0, \quad 2\,u_x\,u_{xxx} - 2\,u_{xx}^2 - 4\,u_{xx} = 0, \quad \ldots \tag{1}$$

Observe that the second equation factors: $2\,u_x\,u_{xx} - 4\,u_x = 2\,u_x\,(u_{xx} - 2)$. The second rule implies that any solution of the system annihilates either the first or the second factor. Thus the system is equivalent to the disjunction:

$$\left\{ \begin{array}{l} u_x^2 - 4\,u = 0, \\ u_x = 0 \end{array} \right. \quad \text{or} \quad \left\{ \begin{array}{l} u_x^2 - 4\,u = 0, \\ u_{xx} - 2 = 0 \end{array} \right.$$

If one solves these systems by means of Analysis, one actually gets two solutions of the initial equation: the zero function $u(x) = 0$ and the family of parabolas $u(x) = (x+c)^2$ where $c$ is some constant. With the wording of Analysis, the first rule implies that one needs to look for solutions in terms of smooth functions (over some open set which would need to be precised). This is a restriction: consider the function $f(x)$ of one real variable, which is zero over $\mathbb{R}^-$ and equal to $x^2$ over $\mathbb{R}^+$. It is only differentiable once at $x = 0$. If one looks for solutions

over some open set containing zero, this solution is lost. Our second example is given by the "differential" equation

$$u\,v = 0$$

of the differential polynomial ring $\mathbb{Q}\{u, v\}$ endowed with the derivation $\delta_x = \partial/\partial x$. Applying the second inference rule, one sees that it is equivalent to:

$$u = 0 \quad \text{or} \quad v = 0.$$

Now, consider the function $f(x)$ of one real variable, which is zero over $\mathbb{R}^-$ and equal to $e^{-\frac{1}{x^2}}$ over $\mathbb{R}^+$ and the function $g(x)$ the graph of which is symmetrical to that of $f(x)$ w.r.t. the ordinates axis. These two functions are smooth but non analytic over any open set containing zero. Over any such open set, the pair $(f(x), g(x))$, which is a solution of the initial equation, does not annihilate any of the two systems produced after the *splitting cases* process: it is lost.

**Summary 1**

- *The algebraic structures $G$ in which one seeks solutions for $\Sigma$ must be $K$-algebras, differential (one needs to be able to differentiate their elements infinitely many times) and integral domains.*
- *Whatever the differential polynomial $p \in \sqrt{[\Sigma]}$ the systems $\Sigma$ and $\Sigma \cup \{p\}$ have the same set of solutions.*

# 4 Abstract solutions

**Theorem and definition 1** *Define an* abstract solution *of $\Sigma$ as a pair:*

1. *a differential field extension $G$ of $K$,*
2. *a $n$-tuple $(\overline{u}_1, \ldots, \overline{u}_n) \in G^n$ which annihilates the elements of $\Sigma$.*

*Then a differential polynomial $p \in R$ vanishes over all the abstract solutions of $\Sigma$ if and only if $p \in \sqrt{[\Sigma]}$. In particular, $\Sigma$ has no abstract solution if and only if $1 \in [\Sigma]$.*

**Proof** See [32, chap. II, sect. 7] or [11, sect. 1.4]. The implication from right to left is immediate, using the arguments given in Summary 1. For the implication from left to right, consider a differential polynomial $p \notin \sqrt{[\Sigma]}$. One needs to show that $\Sigma$ admits an abstract solution which does not annihilate $p$. Theorem 1 implies that there exists a prime differential ideal $\mathfrak{p}$ which contains $\Sigma$ but not $p$. The ring $R/\mathfrak{p}$ is a domain since $\mathfrak{p}$ is prime. It is differential since $\mathfrak{p}$ is differential. Take for $G$ the ring of fractions of the residue class ring $R/\mathfrak{p}$ and for $\overline{u}_1, \ldots, \overline{u}_n$ the images of the differential indeterminates by the natural ring homomorphism $R \to G$. Evaluating a differential polynomial at $\overline{u}_1, \ldots, \overline{u}_n$ amounts to taking its image by $\phi$. The elements of $\Sigma$ are mapped to zero. The polynomial $p$ is mapped to some nonzero element of $G$. $\square$

Abstract solutions are very satisfactory from an algebraic point of view but, in practice, one would like to interpret the abstract derivations as derivations w.r.t. independent variables ($\delta_i = \partial/\partial x_i$) and one would like solutions to be $n$-tuples of "functions" of $m$ variables $u_j(x_1, \ldots, x_m)$. This is done in section 7 but first, one introduces *characteristic sets*, *normal forms* and *purely algebraic solutions* of differential ideals.

# 5 Characteristic sets and normal forms

**Definition 1** *A* ranking *is a total ordering over $\Theta U$ which satisfies the two following axioms:*

1. *$v \leq \theta v$ for every $v \in \Theta U$ and $\theta \in \Theta$,*
2. *$v < w \Rightarrow \theta v < \theta w$ for every $v$, $w \in \Theta U$ and $\theta \in \Theta$.*

See [18, chap. I, sect. 8]. Rankings such that $\operatorname{ord}\theta < \operatorname{ord}\phi \Rightarrow \theta u < \phi v$ for every $\theta$, $\phi \in \Theta$ and $u$, $v \in U$ are called *orderly*. Rankings such that $\theta u < \phi u \Rightarrow \theta v < \phi v$ for every $\theta$, $\phi \in \Theta$ and $u$, $v \in U$ are called *Riquier*. These two special types of rankings will be especially useful in section 8.

Fix a ranking. Consider some differential polynomial $p \notin K$. The highest derivative $v$ w.r.t. the ranking such that $\deg(p, v) > 0$ is called the *leading derivative* of $p$. It is denoted $\operatorname{ld} p$. The leading coefficient of $p$ w.r.t. $v$ is called the *initial* of $p$. The differential polynomial $\partial p/\partial v$ is called the *separant* of $p$. If $C$ is a finite subset of $R \setminus K$ then $I_C$ denotes its set of initials, $S_C$ denotes its set of separants and $H_C = I_C \cup S_C$.

A differential polynomial $q$ is said to be *partially reduced* w.r.t. $p$ if it does not depend on any proper derivative of the leading derivative $v$ of $p$. It is said to be *reduced* w.r.t. $p$ if it is partially reduced w.r.t. $p$ and $\deg(q, v) < \deg(p, v)$. A set of differential polynomials of $R \setminus K$ is said to be *autoreduced* if its elements are pairwise reduced. Autoreduced sets are necessarily finite [18, chap. I, sect. 9]. To each autoreduced set $C$, one may associate the set $L = \operatorname{ld} C$ of the leading derivatives of $C$ and the set $N = \Theta U \setminus \Theta L$ of the derivatives which are not derivatives of any element of $L$ (the derivatives "under the stairs" defined by $C$).

**Example.** The following system $C$

$$v_{xx} - u_x, \quad v_y - \frac{u_x\, u_y}{4}, \quad u_x^2 - 4\, u, \quad u_y^2 - 2\, u$$

is autoreduced w.r.t. the Riquier orderly ranking:

$$u < v < u_y < u_x < v_y < v_x < u_{yy} < u_{xy} < u_{xx} < v_{yy} < \cdots$$

The set of leading derivatives is $L = \{v_{xx},\, v_y,\, u_x,\, u_y\}$. The set of the derivatives which are not derivatives of any element of $L$ is $N = \Theta U \setminus \Theta L = \{u,\, v,\, v_x\}$. It turns out to be finite here.

Ritt's reduction algorithm is a generalization for differential polynomials of the classical *pseudoremainder* algorithm (prem) defined in [17, vol. 2, page 407]. Ritt's algorithm is presented in [18, chap. I, sect. 9]. Given a differential polynomial $p$ and an autoreduced set $C$, it permits to compute a set of exponents $a_1, \ldots, a_t \in \mathbb{N}$ and a differential polynomial $p'$ partially reduced w.r.t. $C$ (i.e. w.r.t. each element of $C$) such that $s_1^{a_1} \cdots s_t^{a_t}\, p \equiv p' \mod [C]$ where $s_1, \ldots, s_t$ denote the separants of the elements of $C$. Given a differential polynomial $p'$ partially reduced w.r.t. $C$, it permits to compute a set of exponents $b_1, \ldots, b_t \in \mathbb{N}$ and a differential polynomial $p''$ reduced w.r.t. $C$ such that $\imath_1^{b_1} \cdots \imath_t^{b_t}\, p' \equiv p''$ mod $(C)$ where $i_1, \ldots, i_t$ denote the initials of the elements of $C$. When $p'' = 0$ one says that $p'$ *is reduced to zero by* $C$.

**Definition 2** *Let $\mathfrak{A}$ be a differential ideal of $R$. A non empty subset $C$ of $\mathfrak{A}$ is said to be a* characteristic set *of $\mathfrak{A}$ if it is autoreduced and $\mathfrak{A}$ involves no nonzero element reduced w.r.t. $C$.*

Every radical differential ideal can be decomposed as a finite intersection of differential ideals $\mathfrak{A}_i$ defined by characteristic sets $C_i$. Algorithms performing this task are described in [7, 22, 13]. The characteristic sets produced by these algorithms hold an extra property: $\mathfrak{A}_i = [C_i] : H_{C_i}^\infty$. They are called *characterizable* in [13]. The next lemma is well-known.

**Lemma 1** *If $C$ is a characteristic set of a differential ideal $\mathfrak{A}$ of $R$ then every element of $\mathfrak{A}$ is reduced to zero by $C$. If moreover $\mathfrak{A} = [C] : H_C^\infty$ then every element of $R$ reduced to zero by $C$ is an element of $\mathfrak{A}$.*

**Proof** Let $p \in \mathfrak{A}$ be reduced to $p'$ by $C$. Then $p' \in \mathfrak{A}$ and is reduced w.r.t. $C$. It is thus zero. Let $p \in R$ be reduced to zero by $C$. Then there exists a power product $h$ of initials and separants of $C$ such that $h\, p \in \mathfrak{A}$. If $\mathfrak{A} = [C] : H_C^\infty$ then $p \in \mathfrak{A}$ according to the definition of saturations. □

**Lemma 2** *Let $C$ be a characteristic set of the differential ideal $[C] : H_C^\infty$. Denote $L = \mathrm{ld}\, C$ and $N = \Theta U \setminus \Theta L$. Then, in the ring $K(N)[L]$, the ideals $(C)$ and $(C) : H_C^\infty$ are equal.*

**Proof** Denote $C = \{c_1, \ldots, c_t\}$. Assume $\mathrm{ld}\, c_1 < \cdots < \mathrm{ld}\, c_t$. For each $1 \leq k < t$, denote $C_k = \{c_1, \ldots, c_k\}$. Let us first place ourselves in the ring $R$. The ideal $(C) : H_C^\infty$ is radical by Lazard's lemma. See [6, Lemma 2], [26] or [9, Corollary 3.3]. Thus by [13, Proposition 3.3], the ideals $(C) : I_C^\infty$ and $(C) : H_C^\infty$ are equal. The set $C$ is a characteristic set, in the non differential sense, of $(C) : I_C^\infty$ since it is a characteristic set of $[C] : H_C^\infty$ and $(C) : I_C^\infty \subset [C] : H_C^\infty$. According to [1, Theorem 6.1], $C$ is thus a regular chain [9, Definition 3.1] whence the initial $i_k$ of $c_k$ is regular modulo the ideal $(C_{k-1}) : I_{C_{k-1}}^\infty$ for each $2 \leq k \leq t$. By [9, Corollary 3.2], in the ring $K(N)[L]$, the initial $i_k$ of $c_k$ is thus invertible modulo the ideal $(C_{k-1}) : I_{C_{k-1}}^\infty$, for each $2 \leq k \leq t$. Let us now place ourselves in $K(N)[L]$. The initial of $c_1$ lies in $K(N)$ and is invertible. Thus $(C_1) = (C_1) : I_{C_1}^\infty$. Assume that, for some $1 < k \leq t$ one has $(C_{k-1}) = (C_{k-1}) : I_{C_{k-1}}^\infty$. Then $i_k$ is

invertible modulo $(C_{k-1})$ and $(C_k) : I_{C_k}^\infty = (C_k)$. Putting the above argument in an inductive proof, the lemma is proven. □

**Definition 3** *Let $C$ be an autoreduced set, $L = \mathrm{ld}\, C$ and $N = \Theta U \setminus \Theta L$. Let $h$ be an initial or a separant of some element of $C$. If $h \in K$ then a* pseudoinverse pair *of $h$ is defined as $(1/h,\, 1)$ else it is defined as any pair $(p,\, q)$ of nonzero differential polynomials such that $p \in K[N \cup L]$, $q \in K[N]$ and $h\, p \equiv q \mod (C)$.*

**Proposition 1** *Take the same notations as in definition 3 and assume moreover that $C$ is a characteristic set of $[C] : H_C^\infty$. Then every initial or separant $h$ of $C$ admits a pseudoinverse pair.*

**Proof** One only needs to consider the case $h \notin K$. Since $h \in H_C$, it is regular modulo $(C) : H_C^\infty$ in the ring $K[N \cup L]$. By [9, Theorem 1.1 and Corollary 1.15], it is thus invertible modulo $(C) : H_C^\infty$ in the ring $K(N)[L]$. In this ring, $(C) = (C) : H_C^\infty$ by Lemma 2 whence there exists a polynomial $r$ such that $r\, h - 1 \in (C)$. Multiplying by some suitable nonzero polynomial $q \in K[N]$ in order to clear denominators and denoting $p = r\, q$, one gets a relation $p\, h - q \in (C)$ in $K[N \cup L]$ hence a pseudoinverse pair $(p,\, q)$ of $h$. □

Proposition 1 is essentially algorithmic since pseudoinverse pairs can be computed by means of the function *algebraic_inverse* given in [9] which is based on [25]. The restriction comes from the fact that this function may fail to compute the inverse of $h$ though $h$ is invertible for it needs to check the regularity of polynomials different from $h$. If such a failure occurs, the characteristic set $C$ can be split as two smaller characteristic sets and the whole process restarted over these ones, following the "$D^5$ principle".

**Example (continued).** The separant of $u_x^2 - 4\, u$ is $2\, u_x$. A pseudoinverse pair of $2\, u_x$ is $(u_x,\, 8\, u)$. The function *algebraic_inverse* of [9] would obtain it by computing a Bézout identity between $2\, u_x$ and $u_x^2 - 4\, u$ in the ring $\mathbb{Q}(u)[u_x]$.

**Proposition 2** *The function* NF *given in Figure 1 returns a rational fraction $f/g$ satisfying the following properties:*

1. *$f$ is reduced w.r.t. $C$,*
2. *$g \in K[N]$ and all its irreducible factors divide the second component of the pseudoinverse pair of some initial or separant of $C$,*
3. *$g$ is regular modulo $\mathfrak{A}$,*
4. *$g\, p \equiv f \mod \mathfrak{A}$,*
5. *for all $p,\, p' \in R$, one has $p \equiv p' \mod \mathfrak{A}$ iff $\mathrm{NF}(p, C) = \mathrm{NF}(p', C)$,*
6. *for all $p \in R$, one has $p \in \mathfrak{A}$ iff $\mathrm{NF}(p, C) = 0$.*

function NF($p$, $C$)
*Assumptions*
*$p$ is a differential polynomial of $R$*
*$C = \{c_1, \ldots, c_t\}$ is a characteristic set of $\mathfrak{A} = [C] : H_C^\infty$*
*One assumes that pseudoinverse pairs of the initials and separants of the elements of $C$ can be computed (see the remark following Proposition 1).*
begin
denote $s_1, \ldots, s_t$ the separants of the elements of $C$
denote $(p_i, q_i)$ a pseudoinverse pair of $s_i$ $(1 \leq i \leq t)$
using Ritt's reduction algorithm, compute $a_1, \ldots, a_t \in \mathbb{N}$ and
$r_{t+1} \in K[N \cup L]$ such that $s_1^{a_1} \cdots s_t^{a_t}\, p \equiv r_{t+1} \mod \mathfrak{A}$
$f_{t+1} := p_1^{a_1} \cdots p_t^{a_t}\, r_{t+1}$
$g_{t+1} := q_1^{a_1} \cdots q_t^{a_t}$
denote $v_i = \operatorname{ld} c_i$ $(1 \leq i \leq t)$ and assume $v_t > \cdots > v_1$
for $\ell$ from $t$ to 1 by $-1$ do
$r_\ell := \operatorname{prem}(f_{\ell+1}, c_\ell, v_\ell)$
denote $(p_\ell, q_\ell)$ a pseudoinverse pair of the initial $i_\ell$ of $c_\ell$
let $a_\ell \in \mathbb{N}$ be such that $i_\ell^{a_\ell}\, f_{\ell+1} \equiv r_\ell \mod (c_\ell)$
$f_\ell := p_\ell^{a_\ell}\, r_\ell$
$g_\ell := q_\ell^{a_\ell}\, g_{\ell+1}$
od
return $f_1/g_1$
*One may make the rational fraction irreducible by computing the gcd of $f_1$ and $g_1$ as multivariate polynomials over the field $K$*
end

Figure 1: The NF function

**Proof** Item (1). Denote $C = \{c_1, \ldots, c_t\}$ and $v_i = \operatorname{ld} c_i$ as in Figure 1. Assume $v_t > \cdots > v_1$. The polynomial $r_{t+1}$ is partially reduced w.r.t. $C$. By Proposition 1, the polynomials $p_1, \ldots, p_t$ lie in $K[N \cup L]$ i.e. are partially reduced w.r.t. $C$. Thus $f_{t+1}$ is partially reduced w.r.t. $C$. Let now $t \geq \ell \geq 1$ be a loop index. Assume $f_{\ell+1}$ is partially reduced w.r.t. $C$ and $\deg(f_{\ell+1}, v_k) < \deg(c_k, v_k)$ for each $t \geq k > \ell$. Consider the sequence of instructions of the loop body. By the specifications of the pseudoremainder algorithm, $\deg(r_\ell, v_\ell) < \deg(c_\ell, v_\ell)$. By Proposition 1 and the fact that $\deg(i_\ell, v_\ell) = 0$ one has $\deg(p_\ell, v_\ell) = 0$. Thus $f_\ell$ is partially reduced w.r.t. $C$ and, using the fact that $c_\ell$ does not depend on $v_{\ell+1}, \ldots, v_t$, one has $\deg(f_\ell, v_k) < \deg(c_k, v_k)$ for each $t \geq k \geq \ell$. Putting the above argument in an inductive proof, one sees that $f = f_1$ is partially reduced w.r.t. $C$ and $\deg(f_1, v_k) < \deg(c_k, v_k)$ for each $t \geq k \geq 1$ i.e. that $f$ is reduced w.r.t. $C$.
Item (2). All polynomials $g_i$ are power products of the second components of the pseudoinverse pairs of the initials and separants of $C$. They belong to $K[N]$ by Proposition 1. The final simplification of the rational fraction $f_1/g_1$ may

remove some factors of $g_1$.
Item (3). One assumes that there exists some $\overline{g} \in R$ such that $g\,\overline{g} \in \mathfrak{A}$. One proves that $\overline{g} \in \mathfrak{A}$. The polynomial $\overline{g}$ may be chosen partially reduced w.r.t. $C$ (if not, replace it by its partial remainder w.r.t. $C$). The polynomial $g\,\overline{g}$ is reduced to zero by $C$ (Lemma 1). Since it is partially reduced w.r.t. $C$, the reduction process is purely algebraic hence $g\,\overline{g} \in (C) : I_C^\infty$. By the equidimensionality argument of Lazard's lemma [9, Theorem 1.6], the associated prime ideals of $(C) : I_C^\infty$ do not meet $K[N] \setminus \{0\}$ (the fact that $N$ may be infinite does not raise any theoretical problem since one may restrict $N$ to the derivatives which actually occur in the polynomials). Thus $g$ does not lie in any associated prime ideal of $(C) : I_C^\infty$ and, by [41, chap. IV, §6, Corollary 3], is regular modulo that ideal. Therefore $\overline{g} \in (C) : I_C^\infty \subset \mathfrak{A}$ and the proof of item (3) is complete.
Item (4). At the beginning of the function, $s_1^{a_1} \cdots s_t^{a_t}\, p \equiv r_{t+1} \mod \mathfrak{A}$. Multiplying both sides of the congruence by $p_1^{a_1} \cdots p_t^{a_t}$ and simplifying each $s_i\, p_i$ by $q_i$ according to Proposition 1, one gets the relation $g_{t+1}\, p \equiv f_{t+1} \mod \mathfrak{A}$. Let now $t \geq \ell \geq 1$ be a loop index, consider the sequence of instructions of the loop body and assume that $g_{\ell+1}\, p \equiv f_{\ell+1} \mod \mathfrak{A}$. Multiply both sides of this congruence by $p_\ell^{a_\ell}\, \imath_\ell^{a_\ell}$. On the lefthand-side, replace each $p_\ell\, i_\ell$ by $q_\ell$ according to Proposition 1. On the righthand-side, replace $\imath_\ell^{a_\ell}\, f_{\ell+1}$ by $r_\ell$. Using the fact that $c_\ell \in \mathfrak{A}$ one gets $g_\ell\, p \equiv f_\ell \mod \mathfrak{A}$. Putting the above argument in an inductive proof, item (4) is proven.
Item (5). Denote $f/g = \mathrm{NF}(p, C)$ and $f'/g' = \mathrm{NF}(p', C)$. The implication from left to right. Assume $p \equiv p' \mod \mathfrak{A}$. Then $g\,g'\,p \equiv g\,g'\,p' \mod \mathfrak{A}$. By item (4) $g'\,f - g\,f' \in \mathfrak{A}$. Since $g$, $g' \in K[N]$ by item (2) and $f$, $f'$ are reduced w.r.t. $C$ by item (1), the difference $g'\,f - g\,f'$ is reduced w.r.t. $C$ hence equal to zero by the definition of characteristic sets. Thus $f/g = f'/g'$. The implication from right to left. Assume $f/g = f'/g'$. Then $g'\,f = g\,f'$ hence, by item (4), $g\,g'\,p \equiv g\,g'\,p' \mod \mathfrak{A}$. Since $g$ and $g'$ are regular modulo $\mathfrak{A}$ by item (3), one has $p \equiv p' \mod \mathfrak{A}$ and item (5) is proven.
Item (6) follows from item (5) and the fact that $\mathrm{NF}(0, C) = 0$. □

**Example (continued).** Here are the normal forms of some elements of $\Theta U$, computed with the help of the BLAD libraries over the example. See [2] and [3, chap. 6].

| derivative | normal form | derivative | normal form |
|---|---|---|---|
| $u$ | $u$ | $u_{xx}$ | $2$ |
| $v$ | $v$ | $u_{xy}$ | $u_x\, u_y/(2\, u)$ |
| $u_y$ | $u_y$ | $u_{yy}$ | $1$ |
| $u_x$ | $u_x$ | $v_{xx}$ | $u_x$ |
| $v_y$ | $(1/4)\, u_x\, u_y$ | $v_{xy}$ | $u_y$ |
| $v_x$ | $v_x$ | $v_{yy}$ | $(1/2)\, u_x$ |

# 6 Purely algebraic solutions of differential ideals

**Definition 4** *Let $\mathfrak{A}$ be a differential ideal of the polynomial differential ring $R = K\{U\}$ and $G_0$ be a field extension of $K$. A map $\phi : \Theta U \to G_0$, which extends to a ring homomorphism $K[\Theta U] \to G_0$, is a* purely algebraic solution *of $\mathfrak{A}$ if $\phi$ annihilates all the elements of $\mathfrak{A}$.*

Informally speaking, a purely algebraic solution of a differential ideal $\mathfrak{A}$ is obtained by viewing $\mathfrak{A}$ as a nondifferential ideal of the ring $K[\Theta U]$ and determining a solution of it. The difficulty, which comes from the fact that the set of unknowns is infinite, is overcome by means of the normal form algorithm.

**Lemma 3** *Let $\mathfrak{A}$ be a differential ideal of the polynomial differential ring $R = K\{U\}$ and $G_0$ be a field extension of $K$. Let $C$ be a characteristic set of $\mathfrak{A}$ and $\phi : \Theta U \to G_0$ be a map, which extends to a ring homomorphism $K[\Theta U] \to G_0$. Let $h$ be an initial or a separant of $C$ and $(p, q)$ be a pseudoinverse pair of $h$. Assume $\phi$ annihilates all the elements of $C$. Then $\phi(h) = 0$ if and only if $\phi(q) = 0$. If $\phi(h) \neq 0$ for each initial or separant $h$ of $C$ then $\phi$ does not annihilate any denominator of* $\mathrm{NF}(R, C)$.

**Proof** Since $h\,p \equiv q \mod (C)$, the first statement is clear. The second statement then follows from item (2) of Proposition 2. □

**Proposition 3** *Let $\mathfrak{A}$ be a differential ideal of $R$ and $C$ be a characteristic set of $\mathfrak{A}$ such that $\mathfrak{A} = [C] : H_C^\infty$. Let $L = \mathrm{ld}\, C$ and $N = \Theta U \setminus \Theta L$. Then any map $\phi$ built as follows provides a purely algebraic solution of $\mathfrak{A}$.*

1. *for all $v \in N \cup L$, assign to $\phi(v)$, values, taken in some field extension $G_0$ of $K$, which annihilate the elements of $C$ but does not annihilate their initials and separants.*

2. *for all $v \in \Theta L \setminus L$, assign then to $\phi(v)$ the value of* $\mathrm{NF}(v, C)$.

**Proof** The map $\phi$ is well-defined. Since $C$ is a characteristic set of $[C] : H_C^\infty$, the ideal $(C) : H_C^\infty$ of the ring $K[N \cup L]$ is not trivial and there exists a prime ideal $\mathfrak{p}$ which contains $C$ and does not contain any element of $H_C$. The field $G_0$ may thus be chosen to be the field of fractions of $K[N \cup L]/\mathfrak{p}$. Since the map $\phi$ does not annihilate the initials and separants of $C$, it does not annihilate any denominator of any element of $\mathrm{NF}(\Theta U, C)$ by Lemma 3. The map $\phi$ is thus well-defined.
The map $\phi$ provides a purely algebraic solution of $\mathfrak{A}$. It is sufficient to prove that, for any $p \in R$ one has $\phi(p - \mathrm{NF}(p, C)) = 0$ since, in the case $p \in \mathfrak{A}$, one has $\mathrm{NF}(p, C) = 0$ by item (6) of Proposition 2 whence $\phi(p) = 0$. Now, $\phi(v - \mathrm{NF}(v, C)) = 0$ for all $v \in \Theta U$. It is thus sufficient to prove that, for all $p, p' \in R$, if $\phi(p - \mathrm{NF}(p, C)) = 0$ and $\phi(p' - \mathrm{NF}(p', C)) = 0$ then $\phi(p + p' - \mathrm{NF}(p + p', C)) = 0$ and $\phi(p\,p' - \mathrm{NF}(p\,p', C)) = 0$. The case of the sum is clear since $\mathrm{NF}(p + p', C) = \mathrm{NF}(p, C) + \mathrm{NF}(p', C)$. Let us prove that $\phi(p\,p' - \mathrm{NF}(p\,p', C)) = 0$. One has $\mathrm{NF}(p\,p', C) \equiv \mathrm{NF}(p, C)\ \mathrm{NF}(p', C)$

mod $\mathfrak{A}$ by item (4) of Proposition 2. Since normal forms are partially reduced w.r.t. $C$, the computation of $\mathrm{NF}(p\,p',\,C)$ from the product $\mathrm{NF}(p,\,C)\,\mathrm{NF}(p',\,C)$ does not imply any differentiation of elements of $C$. Therefore, the congruence $\mathrm{NF}(p\,p',\,C) \equiv \mathrm{NF}(p,\,C)\,\mathrm{NF}(p',\,C) \mod (C) : I_C^\infty$ holds. Since $\phi$ annihilates the elements of $C$ and does not annihilate their initials, one has $\phi(\mathrm{NF}(p\,p',\,C)) = \phi(\mathrm{NF}(p,\,C))\,\phi(\mathrm{NF}(p',\,C))$ hence $\phi(p\,p' - \mathrm{NF}(p\,p',\,C)) = 0$. □

# 7 Formal power series solutions

This section is dedicated to the construction of formal power series solutions of systems of polynomial differential equations. It is the first half of the way leading to analytic solutions. Reference texts for this section are [36, 37]. See also [33, 16]. The $m$ derivations $\delta_1, \ldots, \delta_m$ are interpreted as $m$ partial derivations w.r.t. $m$ independent variables $x_1, \ldots, x_m$. If $\theta = \delta_1^{a_1} \cdots \delta_m^{a_m}$ is a derivation operator, one denotes $x^\theta = x_1^{a_1} \cdots x_m^{a_m}$ and $\theta! = a_1! \cdots a_m!$. One looks for *formal power series solutions* of $\mathfrak{A}$ i.e. solutions of the form:

$$\overline{u}_j = \sum c_{j,\theta} \frac{x^\theta}{\theta!}.$$

The coefficients $c_{j,\theta}$ belong to some field extension $G_0$ of $K$ which depends on the considered system $\Sigma$ or, more simply, in the field $\mathbb{C}$. First remark: the above formal power series is centered on the origin for simplicity but the arguments hold for formal power series centered on any element of $\mathbb{R}^m$. Second remark: the above setting covers also the case of differential systems with coefficients in the field $\mathbb{Q}(x_1, \ldots, x_m)$. Indeed, it is then sufficient to encode each independent variable $x_i$ as a new differential indeterminate $z_i$ and to append to the system under study, the equations $\delta_j\, z_i = 1$ if $i = j$ and 0 otherwise. One thus assumes w.o.l.o.g. that $K$ is a field of constants.

**Proposition 4** *Let $G_0$ be a field extension of $K$ and $\phi : \Theta U \to G_0$ be a map, extending to a ring homomorphism $K[\Theta U] \to G_0$. Then $\phi$ is a purely algebraic solution of $\mathfrak{A}$ if and only if the $n$–tuple $\overline{u} = (\overline{u}_1, \ldots, \overline{u}_n)$ is a formal power series solution of $\mathfrak{A}$ where*

$$\overline{u}_j = \sum_{\theta \in \Theta} \phi(\theta u_j)\, \frac{x^\theta}{\theta!}, \quad 1 \leq j \leq n.$$

*Moreover, for each differential polynomial $p \in R$, if $\phi(p) \neq 0$ then $p(\overline{u}) \neq 0$.*

**Proof** See [36, Lemma]. If $p \in R$ is a differential polynomial then $p(\overline{u}) = \sum \phi(\theta p)\, x^\theta/\theta!$. Therefore $p(\overline{u})$ is zero if and only if $\phi(\theta p)$ is zero for all $\theta \in \Theta$. Thus $\phi$ is a purely algebraic solution of $\mathfrak{A}$ if and only if $\overline{u}$ is a formal power series solution of $\mathfrak{A}$. The last part of the proposition is clear. □

**Example (continued).** One illustrates the proposition over the example of section 5. The map $\phi$ should be understood as the evaluation over the expansion point of the series i.e. $\phi(w) = w(0,0)$ for any derivative $w$. One assigns to $u(0,0)$ any nonzero value (since $u$ is a denominator of $\mathrm{NF}(\Theta U, C)$ and must not vanish). One assigns to $v(0,0)$ and $v_x(0,0)$ any value. The values assigned to $u_x(0,0)$ and $u_y(0,0)$ must then be compatible with the equations of $C$ (differential equations, which impose equalities between functions, must be satisfied for all values of $x$ and $y$ hence, in particular, for $x = y = 0$). The equations to be satisfied are:

$$u_x(0,0)^2 - 4\,u(0,0) = 0, \quad u_y(0,0)^2 - 2\,u(0,0) = 0.$$

Let us thus choose three arbitrary constants $c_0$, $c_1$, $c_2 \in \mathbb{R}$ such that $c_0 \neq 0$ and $c_1$, $c_2 \geq 0$ then let

$$(u(0,0),\, v(0,0),\, v_x(0,0),\, u_x(0,0),\, u_y(0,0)) = (c_0,\, c_1,\, c_2,\, 2\sqrt{c_0},\, \sqrt{2\,c_0}).$$

The values assigned to all the other derivatives $w$ are then uniquely determined for we have:

$$w(0,0) = \mathrm{NF}(w, C)(0,0).$$

It turns out that all normal forms of derivatives are identically zero at some order hence that the formal power series solutions are polynomials:

$$\begin{aligned} u(x,y) &= c_0 + 2\sqrt{c_0}\,x + \sqrt{2\,c_0}\,y + x^2 + \sqrt{2}\,x\,y + \frac{1}{2}\,y^2, \\ v(x,y) &= c_1 + c_2\,x + \frac{\sqrt{2}\,c_0}{2}\,y + \sqrt{c_0}\,x^2 + \sqrt{2\,c_0}\,x\,y + \frac{\sqrt{c_0}}{2}\,y^2 \\ &+ \frac{1}{3}\,x^3 + \frac{\sqrt{2}}{2}\,x^2\,y + \frac{1}{2}\,x\,y^2 + \frac{\sqrt{2}}{12}\,y^3. \end{aligned}$$

**Theorem and definition 2** *Define a* formal power series solution *of* $\Sigma$ *as a pair:*

1. *a field extension* $G_0$ *of* $K$*,*
2. *a* $n$*-tuple* $(\overline{u}_1, \ldots, \overline{u}_n) \in G = G_0[[x_1, \ldots, x_m]]^n$ *which annihilates the elements of* $\Sigma$*.*

*Then a differential polynomial* $p \in R$ *vanishes over all the formal power series solutions of* $\Sigma$ *if and only if* $p \in \sqrt{[\Sigma]}$*. In particular,* $\Sigma$ *has no formal power series solution if and only if* $1 \in [\Sigma]$*.*

**Proof** The implication from right to left is immediate using the arguments given in Summary 1. For the implication from left to right, consider some differential polynomial $p \notin \sqrt{[\Sigma]}$. One needs to show that $\Sigma$ admits a formal power series solution which does not annihilate $p$. Theorem 1 implies that there exists some prime differential ideal $\mathfrak{p}$ which contains $\Sigma$ but not $p$. This ideal admits characteristic sets w.r.t. any ranking. Let $C$ be one of them. Since $\mathfrak{p}$ is prime, $\mathfrak{p} = [C] : H_C^\infty$ [32, chap. II, §5] and one may apply Proposition 3. The

map $\phi$ may be chosen so that $\phi(\mathrm{NF}(p,\, C)) \neq 0$ whence $\phi(p) \neq 0$, taking e.g. $G_0$ to be the field of fractions of $K[N \cup L]/(\mathfrak{p} \cap K[N \cup L])$. By Proposition 4, the map $\phi$ provides a formal power series solution of $\Sigma$ which does not annihilate $p$. $\square$

# 8 Analytic solutions

Let us proceed on the second half of the way started in the former section and address the case of analytic solutions i.e. formal power series solutions which converge in some open set $\mathscr{D}$. The proof of the Theorem and Definition 3 is split into Propositions 5 and 7.

**Proposition 5** *Assume that every prime differential ideal of $R$ admits an analytic solution. Then, for each $p \in R$, if $p \notin \sqrt{[\Sigma]}$ then $\Sigma$ admits an analytic solution which does not annihilate $p$.*

**Proof** By Theorem 1, it is sufficient to show that, if $\mathfrak{p}$ is a prime differential ideal and $p \notin \mathfrak{p}$ then $\mathfrak{p}$ admits an analytic solution which does not annihilate $p$. Consider the differential ideal $[\mathfrak{p},\, p\, u_{n+1} - 1]$ where $u_{n+1}$ is some new differential indeterminate. This ideal admits abstract solutions (as well as formal power series solutions) according to the hypotheses and one of the already proven differential theorems of zeros. It is thus different from the unit ideal and is contained in some prime differential ideal $\mathfrak{p}'$ of $R\{u_{n+1}\}$. On the one hand, no solution of $\mathfrak{p}'$ annihilates $p$. On the other hand, there is a bijection between the solutions of $\mathfrak{p}'$ and the solutions of $\mathfrak{p}$ which do not annihilate $p$. Since every prime differential ideal admits an analytic solution, $\mathfrak{p}'$ admits an analytic solution, and $\mathfrak{p}$ admits an analytic solution which does not annihilate $p$. $\square$

The fact that every prime differential ideal admits an analytic solution is proven in Proposition 7. This result is known since the work [31] of Riquier. Riquier's theorem, which is a generalization of the Cauchy-Kovalevska theorem, is the basis of [32, chap. VIII] and of the Embedding Theorem [36, 37] of Seidenberg. Germa [28] clarified the relationship between characteristic sets and the hypotheses of Riquier's theorem. More recently, Lemaire [20] completely proved this latter anew, by using a more modern formalism and by distinctly separating the proof of the existence of formal power series solutions and the analyticity proof. The key result is

**Proposition 6** *Let $C$ be a characteristic set defining some prime differential ideal $\mathfrak{p}$, for some orderly Riquier ranking. Let $L$ be the set of the leading derivatives of $C$ and $N = \Theta U \setminus \Theta L$. Let $(\overline{u}_1, \ldots, \overline{u}_n)$ be a formal power series solution of $\mathfrak{p}$, the coefficients $c_{j,\theta}$ lying in the field of the complex numbers. Let $(\tilde{u}_1, \ldots, \tilde{u}_n)$ be the restriction to $N$ of the solution i.e:*

$$\tilde{u}_j = \sum_{\theta \in \Theta} \tilde{c}_{j,\theta} \frac{x^\theta}{\theta!}, \quad 1 \leq j \leq n$$

*defined by* $\tilde{c}_{j,\theta} = c_{j,\theta}$ *if* $\theta u_j \in N$ *else zero. In the neighborhood of the origin, the series* $\tilde{u}_j$ *are analytic if and only if the series* $\overline{u}_j$ *are analytic.*

**Proof** See [20, Théorème d'analyticité, page 50]. □

**Proposition 7** *Every prime differential ideal admits an analytic solution.*

**Proof** Let $\mathfrak{p}$ be some prime differential ideal. Let $C$ be some characteristic set of $\mathfrak{p}$, for some orderly Riquier ranking. Let $L$ be the set of the leading derivatives of $C$ and $N = \Theta U \setminus \Theta L$. Among all the purely algebraic solutions of $\mathfrak{p}$, choose one such that *only finitely many* nonzero values are assigned to the elements of $L \cup N$ (there is no theoretical difficulty since there are only finitely many derivatives occuring in $C$). The restrictions to $N$ of these formal power series are analytic since they are polynomials. According to Proposition 6, the formal power series are analytic whence $\mathfrak{p}$ admits an analytic solution. □

Let us illustrate Proposition 6 over some famous linear example (historically, this is the very example used by Sophie Kovalevska to show the importance of expressing the most differentiated derivatives in terms of the other ones i.e. the importance of the orderly rankings): the heat equation

$$\frac{\partial^2 u}{\partial x^2} = \frac{\partial u}{\partial t}.$$

This equation forms a characteristic set of the prime differential ideal that it generates, whatever the ranking. Over this example, the only thing which depends on the ranking is the leading derivative of the equation. If the ranking is orderly then the leading derivative is $\partial^2 u/\partial x^2$ else it is $\partial u/\partial t$. The purely algebraic solution

$$\frac{\partial^{k+\ell} u}{\partial x^k \partial t^\ell} \mapsto (k+2\ell)!$$

of the heat equation provides a formal power series solution

$$u(x,t) = \sum \frac{(k+2\ell)!}{k!\,\ell!}\, x^k\, t^\ell.$$

For $x > 0$ and $t > 0$, the series does not converge since it grows faster than the well-known divergent series:

$$\sum \ell!\, t^\ell.$$

However, the restriction to

$$N = \left\{ \frac{\partial^k u}{\partial x^k} \mid k \geq 0 \right\}$$

of the formal power series is indeed a convergent series:

$$u(x,0) = \sum x^k = \frac{1}{1-x}.$$

The proposition (indeed, the Cauchy-Kovalevska theorem is sufficient here) tells us that this does not happen if the leading derivative is $\partial^2 u/\partial x^2$. The following example, borrowed from [19], shows the importance of Riquier rankings:

$$\frac{\partial^2 u}{\partial x^2} = \frac{\partial^2 u}{\partial x\,\partial t} + \frac{\partial^2 u}{\partial t^2} + v, \quad \frac{\partial^2 v}{\partial t^2} = \frac{\partial^2 v}{\partial x\,\partial t} + \frac{\partial^2 v}{\partial x^2} + u.$$

One chooses the lefthand sides of the equations as leading derivatives. This is possible only if the chosen ranking is not Riquier. The ranking may however be orderly. The set $N$ is formed of the derivatives of $u$ differentiated at most once w.r.t. $c$ and of the derivatives of $v$ differentiated at most once w.r.t. $t$. One can form a formal power series solution $(\overline{u}, \overline{v})$ whose restriction to $N$ is defined by

$$\overline{u}(0,t) = \frac{\partial u}{\partial x}(0,t) = e^t, \quad \overline{v}(x,0) = \frac{\partial v}{\partial t}(x,0) = e^x.$$

It can be established that the formal power series $\overline{u}$ and $\overline{v}$ are not analytic in the neighborhood of the origin. However their restrictions to $N$ are analytic.

**Theorem and definition 3** *Define an analytic solution of $\Sigma$ as a $n$-tuple of functions $(\overline{u}_1, \ldots, \overline{u}_n)$ of $m$ real or complex variables, analytic over some open set $\mathscr{D}$.*

*Then a differential polynomial $p \in R$ vanishes over all the analytic solutions of $\Sigma$ if and only if $p \in \sqrt{[\Sigma]}$. In particular, $\Sigma$ has no analytic solution if and only if $1 \in [\Sigma]$.*

**Proof** By Propositions 5 and 7. □

For functions of $m$ complex variables, the following properties are equivalent: being differentiable once (i.e. being holomorphic), being smooth and being analytic. This is not the case for functions of $m$ real variables (cf. the examples given at the beginning of this paper). It is worth noticing that the theorem of zeros also holds for smooth functions of $m$ real variables. Indeed, if $p \in \sqrt{[\Sigma]}$ then every smooth solution of $\Sigma$ is a solution of $p$ (first, this is immediate if $p$ lies in the differential ideal generated by $\Sigma$; second, if a power of a smooth function $f$ is zero over some open set then $f$ itself is zero over this set). Conversely, if $p \notin \sqrt{[\Sigma]}$ then $\Sigma$ admits an analytic solution (hence a smooth solution) which does not annihilate $p$. *It is the splitting cases mechanism* implemented in the algorithms cited in the introduction *which does not apply* to smooth functions of $m$ real variables. Last, observe that the theorem of zeros forces us to search analytic solutions with images in the field of the complex numbers but not necessarily analytic functions of $m$ complex variables. As an example, consider the "differential" equation $u^2 + 1 = 0$. It admits for solutions the constant functions $u(x) = \pm i$. These functions have images in $\mathbb{C}$ but the variable $x$ may be real as well as complex.

# 9 On Denef and Lipshitz undecidability result

As shown in section 7, one can compute formal power series solutions of differential ideals defined by characteristic sets for all initial conditions (or purely

algebraic solutions) which do not annihilate some finite set of polynomials. This restriction on admissible initial conditions is sometimes superfluous. Sometimes it is not, the following theorem shows, which is an almost immediate consequence of the undecidability result [12, Theorem 4.11].

**Theorem 2** *The problem "given a characteristic set $C$ and an expansion point $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{Q}^m$, determine if the differential ideal defined by $C$ admits a formal power series solution centered on $\alpha$" is undecidable for $m \geq 9$.*

**Proof** The proof starts exactly as in [12]. Let $P \in \mathbb{Z}[a_1, \ldots, a_m]$ be a polynomial and $u$ be a differential indeterminate. The next expression defines a linear partial differential equation[1]:

$$P\left(x_1 \frac{\partial}{\partial x_1}, \ldots, x_m \frac{\partial}{\partial x_m}\right) u \quad = \quad 0. \tag{2}$$

First remark: if one substitutes a formal power series

$$\overline{u} = \sum_{a_1, \ldots, a_m} c_{a_1, \ldots, a_m} x_1^{a_1} \cdots x_m^{a_m}$$

whose coefficients are still to be determined in equation (2), one gets an expression:

$$P\left(x_1 \frac{\partial}{\partial x_1}, \ldots, x_m \frac{\partial}{\partial x_m}\right) \overline{u} \quad = \quad \sum_{a_1, \ldots, a_m} c_{a_1, \ldots, a_m} P(a_1, \ldots, a_m)\, x_1^{a_1} \cdots x_m^{a_m}.$$

Second remark:

$$\sum_{a_1, \ldots, a_m} x_1^{a_1} \cdots x_m^{a_m} = \left(\frac{1}{1 - x_1}\right) \cdots \left(\frac{1}{1 - x_m}\right).$$

Combining both remarks, one concludes that, the following partial differential equation

$$P\left(x_1 \frac{\partial}{\partial x_1}, \ldots, x_m \frac{\partial}{\partial x_m}\right) u \quad = \quad \left(\frac{1}{1 - x_1}\right) \cdots \left(\frac{1}{1 - x_m}\right)$$

has a formal power series solution $\overline{u}$ (which, if it exists, is necessarily convergent) if and only if the coefficients $c_{a_1, \ldots, a_m}$ satisfy:

$$c_{a_1, \ldots, a_m} = \frac{1}{P(a_1, \ldots, a_m)}$$

[1] Let us develop an example for casual readers. Take $P(a_1, a_2) = 3\, a_1^2 + 2\, a_2$. Then

$$\begin{aligned} P\left(x_1 \frac{\partial}{\partial x_1}, x_2 \frac{\partial}{\partial x_2}\right) u \quad &= \quad 3\, x_1 \frac{\partial}{\partial x_1} \left(x_1 \frac{\partial}{\partial x_1} u\right) + 2 \left(x_2 \frac{\partial}{\partial x_2}\right) u \\ &= \quad 3\, x_1 \frac{\partial}{\partial x_1} (x_1\, u_{x_1}) + 2\, x_2\, u_{x_2} \\ &= \quad 3\, x_1^2\, u_{x_1 x_1} + 3\, x_1\, u_{x_1} + 2\, x_2\, u_{x_2}. \end{aligned}$$

whence $P(a_1, \ldots, a_m) \neq 0$ for all $(a_1, \ldots, a_m) \in \mathbb{N}^m$. According to a celebrated theorem [24] of Matijasevic, the problem of determining whether a polynomial in $\mathbb{Z}[a_1, \ldots, a_m]$ admits an integer solution is undecidable for $m \geq 9$ (negative answer to Hilbert's tenth problem).

These arguments immediately apply to polynomial differential systems whose coefficients do not depend on the independent variables $x_i$ (the setting of this paper). It is sufficient to encode each independent variable $x_i$ by a differential indeterminate $z_i$ and to consider the following differential system $C$, which is a characteristic set for any ranking $u \gg (z_1, \ldots, z_m)$ such that every derivative of $u$ is greater than any derivative of any $z_i$:

$$\begin{aligned} (1 - z_1) \cdots (1 - z_m)\, P\left(z_1 \frac{\partial}{\partial x_1}, \ldots, z_m \frac{\partial}{\partial x_m}\right) u &= 1 \\ \frac{\partial}{\partial x_j} z_i &= 1 \text{ if } i = j \text{ else } 0. \end{aligned}$$

□

What is the relationship between this theorem and the construction of formal power series solutions detailed in section 7 ? Consider the characteristic set at the bottom of the above proof. All the monomials of the first equation of $C$ admit one of the $z_i$ differential indeterminates as a factor. Therefore, the initial of the first equation of $C$ has the form $z_i^r (1 - z_1) \cdots (1 - z_m)$ where $r$ is a positive integer and $1 \leq i \leq m$ is an index. In order to compute a formal power series solution of $C$, centered at $(\alpha_1, \ldots, \alpha_m) \in \mathbb{R}^m$, one must take care to the fact that the values associated to the derivatives $z_1, \ldots, z_m$ necessarily are the numbers $\alpha_1, \ldots, \alpha_m$. The formal power series defined in [12] is centered at $(\alpha_1, \ldots, \alpha_m) = (0, \ldots, 0)$ however, these initial conditions annihilate the initial of the first equation of $C$. The construction of formal power series solutions, based on Proposition 3 avoid them. There is thus no contradiction between all these results.

# Conclusion

Differential algebra can be generalized in order to handle non commuting derivations. A generalization of Hilbert's differential theorem of zeros holds in this setting in the context of abstract solutions as well as in the context of formal power series solutions. See [15, 21]. However, formulating formal power series solutions by means of some normal form algorithm still needs to be done. Observe also that, to our knowledge, no analogues of the analyticity theorem (our Proposition 6) whence of Hilbert's differential theorem of zeros for analytic solutions are proven in the setting of non commuting derivations. This task is left for the future.

# References


[1] Philippe Aubry, Daniel Lazard, and Marc Moreno Maza. On the theories of triangular sets. *Journal of Symbolic Computation*, 28:105–124, 1999.

[2] François Boulier. The BLAD libraries. `http://www.lifl.fr/~boulier/BLAD`, 2004.

[3] François Boulier. Réécriture algébrique dans les systèmes d'équations différentielles polynomiales en vue d'applications dans les Sciences du Vivant, May 2006. Mémoire d'habilitation à diriger des recherches. Université Lille I, LIFL, 59655 Villeneuve d'Ascq, France. `http://tel.archives-ouvertes.fr/tel-00137153`.

[4] François Boulier. Differential Elimination and Biological Modelling. *Radon Series Comp. Appl. Math.*, 2:111–139, 2007. `http://hal.archives-ouvertes.fr/hal-00139364`.

[5] François Boulier. *Étude et implantation de quelques algorithmes en algèbre différentielle*. PhD thesis, Université Lille I, 59655, Villeneuve d'Ascq, France, 1994. `http://tel.archives-ouvertes.fr/tel-00137866`.

[6] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot. Representation for the radical of a finitely generated differential ideal. In *ISSAC'95: Proceedings of the 1995 international symposium on Symbolic and algebraic computation*, pages 158–166, New York, NY, USA, 1995. ACM Press. `http://hal.archives-ouvertes.fr/hal-00138020`.

[7] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot. Computing representations for radicals of finitely generated differential ideals. Technical report, Université Lille I, LIFL, 59655, Villeneuve d'Ascq, France, 1997. Ref. IT306. December 1998 version published in the HDR memoir of Michel Petitot. `http://hal.archives-ouvertes.fr/hal-00139061`.

[8] François Boulier and François Lemaire. Computing canonical representatives of regular differential ideals. In *ISSAC'00: Proceedings of the 2000 international symposium on Symbolic and algebraic computation*, pages 38–47, New York, NY, USA, 2000. ACM Press. `http://hal.archives-ouvertes.fr/hal-00139177`.

[9] François Boulier, François Lemaire, and Marc Moreno Maza. Well known theorems on triangular systems and the $D^5$ principle. In *Proceedings of Transgressive Computing 2006*, pages 79–91, Granada, Spain, 2006. `http://hal.archives-ouvertes.fr/hal-00137158`.

[10] Driss Bouziane, Abdelillah Kandri Rody, and Hamid Maârouf. Unmixed–Dimensional Decomposition of a Finitely Generated Perfect Differential Ideal. *Journal of Symbolic Computation*, 31:631–649, 2001.

[11] Alexandru Buium and Phyllis Cassidy. *Differential Algebraic Geometry and Differential Algebraic Groups: From Algebraic Differential Equations To Diophantine Geometry*, pages 567–636. Amer. Math. Soc., Providence, RI, 1998.

[12] Jan Denef and Leonard Lipshitz. Power Series Solutions of Algebraic Differential Equations. *Mathematische Annalen*, 267:213–238, 1984.

[13] Évelyne Hubert. Factorization free decomposition algorithms in differential algebra. *Journal of Symbolic Computation*, 29(4,5):641–662, 2000.

[14] Évelyne Hubert. Notes on triangular sets and triangulation–decomposition algorithm II: Differential Systems. *Symbolic and Numerical Scientific Computing 2001*, pages 40–87, 2003.

[15] Évelyne Hubert. Differential algebra for derivations with nontrivial commutation rules. *Journal of Pure and Applied Algebra*, 200(1-2):163–190, 2005.

[16] Évelyne Hubert and Nicolas Le Roux. Computing Power Series Solutions of a Nonlinear PDE System. In *Proceedings of ISSAC 2003*, pages 148–155, Philadelphia, USA, 2003.

[17] Donald Erwin Knuth. *The art of computer programming*. Addison–Wesley, 1966. Second edition.

[18] Ellis Robert Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, New York, 1973.

[19] François Lemaire. An orderly linear PDE system with analytic initial conditions with a non analytic solution. *Special Issue on Computer Algebra and Computer Analysis, Journal of Symbolic Computation*, 35(5):487–498, 2003.

[20] François Lemaire. *Contribution à l'algorithmique en algèbre différentielle*. PhD thesis, Université Lille I, 59655, Villeneuve d'Ascq, France, january 2002.

[21] François Lemaire, Greg Reid, and Yang Zhang. Non-commutative riquier theory in moving frames of differential operators. *Submitted to the Journal of Computation and Mathematics*, 2006.

[22] Ziming Li and Dongming Wang. Coherent, regular and simple systems in zero decompositions of partial differential systems. *Systems Science and Mathematical Sciences*, 12:43–60, 1999.

[23] Elizabeth L. Mansfield. *Differential Gröbner Bases*. PhD thesis, University of Sydney, Australia, 1991.

[24] Yu Matijasevic. Enumerable sets are diophantine. *Sov. Math. Dokl.*, 11:354–357, 1970.

[25] Marc Moreno Maza and Renaud Rioboo. Polynomial gcd computations over towers of algebraic extensions. In *Proceedings of AAECC11*, pages 365–382. Springer Verlag, 1995.

[26] Sally Morrison. The Differential Ideal $[P] : M^{\infty}$. *Journal of Symbolic Computation*, 28:631–656, 1999.

[27] Céline Noiret. *Utilisation du calcul formel pour l'identifiabilité de modèles paramétriques et nouveaux algorithmes en estimation de paramètres*. PhD thesis, Université de Technologie de Compiègne, 2000.

[28] Ariane Péladan-Germa. *Tests effectifs de Nullité dans des extensions d'anneaux différentiels*. PhD thesis, École Polytechnique, Palaiseau, France, 1997.

[29] Gregory J. Reid, Ping Lin, and Allan D. Wittkopf. Differential Elimination–Completion Algorithms for DAE and PDAE. *Studies in Applied Mathematics*, 106(1):1–45, 2001.

[30] Gregory J. Reid, Allan D. Wittkopf, and Alan Boulton. Reduction of systems of nonlinear partial differential equations to simplified involutive forms. *European Journal of Applied Math.*, pages 604–635, 1996.

[31] Charles Riquier. *Les systèmes d'équations aux dérivées partielles*. Gauthier–Villars, Paris, 1910.

[32] Joseph Fels Ritt. *Differential Algebra*. Dover Publications Inc., New York, 1950. `http://www.ams.org/online_bks/coll33`.

[33] Colin J. Rust, Gregory J. Reid, and Allan D. Wittkopf. Existence and Uniqueness Theorems for Formal Power Series Solutions of Analytic Differential Systems. In *proceedings of ISSAC 1999*, Vancouver, Canada, 1999.

[34] Abraham Seidenberg. Some basic theorems in differential algebra (characteristic $p$ arbitrary). *Trans. Amer. Math. Soc.*, 73:174–190, 1952.

[35] Abraham Seidenberg. An elimination theory for differential algebra. *Univ. California Publ. Math. (New Series)*, 3:31–65, 1956.

[36] Abraham Seidenberg. Abstract differential algebra and the analytic case. *Proc. Amer. Math. Soc.*, 9:159–164, 1958.

[37] Abraham Seidenberg. Abstract differential algebra and the analytic case II. *Proc. Amer. Math. Soc.*, 23:689–691, 1969.

[38] William Sit. The Ritt–Kolchin theory for differential polynomials. In *proceedings of the international workshop: Differential Algebra and Related Topics*, 2002.

[39] Dongming Wang. *Elimination Practice: Software Tools and Applications*. Imperial College Press, London, 2003.

[40] Wu Wen Tsün. On the foundation of algebraic differential geometry. *Mechanization of Mathematics, research preprints*, 3:2–27, 1989.

[41] Oscar Zariski and Pierre Samuel. *Commutative Algebra*. Van Nostrand, New York, 1958. Also volumes 28 and 29 of the *Graduate Texts in Mathematics*, Springer Verlag.